FS-ISAC | Commercial Services Security Newsletter

December 2024 | CSN Q4-2024

Security is *Everyone's* Responsibility

## Are You Ready for the Holiday Fraud Rush?

**Summary**

The holiday season generally brings out the good in people everyone except threat actors. Fraud and security challenges come in various ways depending on your type of business. Retail companies face fraudulent payment cards, checks, insider fraud, and shoplifting. eCommerce and tech companies face cyber threats including distributed denial of service, phishing, malware, and ransomware attacks.

## Common Fraud Threats

The fraud and security threats facing small businesses continue to increase as threat actors vary their tactics and hone their skills to by-pass changing security tools, below are the most common threats you may face during the 2024 Holiday Season:

## Prevention Measures

- Educate employees by providing training on how to recognize and prevent common types of fraud.
- Use dual controls when processing cash, invoices, and wire transfers. No individual employee should be allowed to create and approve a financial transaction.
- Align payment processes with the Payment Card Industry Data Security Standard (PCI) to protect cardholder personally identifiable information against threat actors.
- Ask your financial institutions which security tools they offer to prevent fraud.
- Identify IT and security employees who would be available during weekends and holidays in the event of an incident or ransomware attack.
    - Implement multi-factor authentication for remote access and administrative accounts.
    - Mandate strong passwords and ensure they are not reused across multiple accounts.
    - If you use remote desktop protocol (RDP) or any other potentially risky service, ensure it is secure and monitored.
- Remind employees not to click on suspicious links, and conduct exercises to raise awareness.
    - Phishing scams, such as unsolicited emails posing as charitable organizations.
    - Fraudulent sites spoofing reputable businesses - it is possible malicious actors may target sites often visited by users doing their holiday shopping online.

    - Unencrypted financial transactions.

- Reduce the risk of severe business/functional degradation should your organization fall victim to a ransomware attack - review and, if needed, update your incident response and communication plans. These plans should list actions to take - and contacts to reach out to - should your organization be impacted by a ransomware incident. Note: for assistance, review available incident response guidance, such as the Ransomware Response Checklist in the Nonbank Ransomware Self-Assessment Tool, and the new Federal Government Cybersecurity Incident and Vulnerability Response Playbooks.

For a comprehensive overview, see the joint Cybersecurity Advisory Ransomware Awareness for Holidays and Weekends. For more information and resources on protecting against and responding to ransomware, visit StopRansomware.gov, a centralized, whole-of-government webpage providing ransomware resources and alerts.

## Be Cyber Smart This Holiday Season!

- Do not provide personal information to any unsolicited requests for information
- Only provide personal information on sites that have "https" in the web address or have a lock icon at the bottom of the browser
- If you suspect you've received phishing bait, contact the company that is the subject of the email by phone to check that the message is legitimate and not an online fraud scam
- Type in a trusted URL for a company's site into the address bar of your browser to bypass the link in a suspected phishing message
- Use varied and complex passwords for all your accounts
  Continually check the accuracy of personal accounts and deal with any discrepancies right away
- Avoid questionable Web sites
- Practice safe email protocol:
    - Don't open messages from unknown senders
    - Immediately delete messages you suspect to be spam
    - Update your operating system regularly
- Make sure that you have the best security software products installed on your PC:
- Use antivirus protection and a firewall
- Get antispyware software protection

## If You Think You've Been Scammed

- Contact your institution immediately so they can act and provide recommendations.
- Report suspicious activity to the Internet Crime Center, www.ic3.com, and/or your local law enforcement agency.

---

TLP WHITE

12120 Sunset Hills Rd, Reston
VA 20190

.